EXHIBIT A

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Thursday, May 19, 2022

Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act

The Department of Justice today announced the revision of its policy regarding charging violations of the Computer Fraud and Abuse Act (CFAA).

The policy for the first time directs that good-faith security research should not be charged. Good faith security research means accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services.

"Computer security research is a key driver of improved cybersecurity," said Deputy Attorney General Lisa O. Monaco. "The department has never been interested in prosecuting good-faith computer security research as a crime, and today's announcement promotes cybersecurity by providing clarity for good-faith security researchers who root out vulnerabilities for the common good."

The new policy states explicitly the longstanding practice that "the department's goals for CFAA enforcement are to promote privacy and cybersecurity by upholding the legal right of individuals, network owners, operators, and other persons to ensure the confidentiality, integrity, and availability of information stored in their information systems." Accordingly, the policy clarifies that hypothetical CFAA violations that have concerned some courts and commentators are not to be charged. Embellishing an online dating profile contrary to the terms of service of the dating website; creating fictional accounts on hiring, housing, or rental websites; using a pseudonym on a social networking site that prohibits them; checking sports scores at work; paying bills at work; or violating an access restriction contained in a term of service are not themselves sufficient to warrant federal criminal charges. The policy focuses the department's resources on cases where a defendant is either not authorized at all to access a computer or was authorized to access one part of a computer — such as one email account — and, despite knowing about that restriction, accessed a part of the computer to which his authorized access did not extend, such as other users' emails.

However, the new policy acknowledges that claiming to be conducting security research is not a free pass for those acting in bad faith. For example, discovering vulnerabilities in devices in order to extort their owners, even if claimed as "research," is not in good faith. The policy advises prosecutors to consult with the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) about specific applications of this factor.

All federal prosecutors who wish to charge cases under the Computer Fraud and Abuse Act are required to follow the new policy, and to consult with CCIPS before bringing any charges. Prosecutors must inform the Deputy Attorney General (DAG), and in some cases receive approval from the DAG, before charging a CFAA case if CCIPS recommends against it.

Ex A, p. 1

The new policy replaces an earlier policy that was issued in 2014, and takes effect immediately.

Attachment(s):
Download CFAA Policy May 2022

Topic(s):
Cybercrime

Component(s):
Criminal Division
Criminal - Computer Crime and Intellectual Property Section
Office of the Deputy Attorney General

Press Release Number:
22-533

Updated May 19, 2022

Ex A, p. 2